

5/7
13

- ii. Certifying that the Business Associate understands that it is required to notify the Nursing Service of any Breach upon discovery of the Breach; and
 - iii. Providing a description or copy of the written information security program followed by the Business Associate.
- D. The Compliance Officer will review policies of all Business Associates to ensure that they are effective in preventing Identity Theft.
- E. The Compliance Officer will provide a copy of this Policy to all Business Associates with a letter requesting that it be followed to the extent it is more stringent than the Business Associates' own policies.
- F. When entering into agreements with new Business Associates or renewing existing contracts, the Nursing Service will ensure that the agreement requires compliance with this Policy.

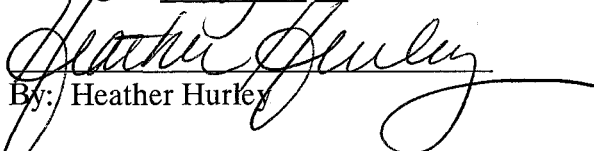
E. APPROVAL AND EFFECTIVE DATE

1. This Policy will take effect immediately upon its approval by the Nursing Service Administrator in consultation with the Group of Professional Personnel, the Board of Health, and the Board of Selectmen.
2. Approval is documented below.

APPROVED:

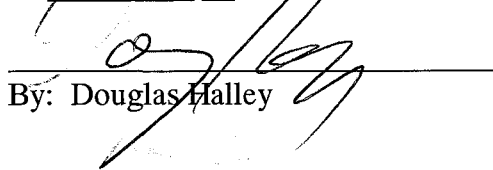
**NURSING SERVICE
ADMINISTRATOR:**

The foregoing Policy was approved by vote of the Group of Professional Personnel at a meeting on May 3, 2012.


By: Heather Hurley

ACTON HEALTH DIRECTOR:

The foregoing Policy was approved by vote of the Board of Health at an open meeting on _____, 2012.


By: Douglas Halley

ACTON BOARD OF SELECTMEN:

The foregoing Policy was approved by vote of the Board of Selectmen at an open meeting on May 7, 2012.

By: Michael Gowing, Clerk

ACTON PUBLIC HEALTH NURSING SERVICE

SUBJECT: Identity Theft Policy

CHAPTER: LEADERSHIP

A. PURPOSES: The purposes of this Policy are:

1. To help protect employees, patients, customers, contractors and the Town of Acton from damages related to the loss or misuse of personal data.
2. To identify, detect and respond to Red Flags indicating possible Identity Theft related to services offered by the Acton Public Health Nursing Service (the "Nursing Service").
3. To ensure the Nursing Service's compliance with the HIPAA Breach Notification Rule.
4. To ensure that this Policy is updated periodically.

B. DEFINITIONS: For the purposes of this Policy, the following definitions apply:

1. "Breach" means an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of protected health information, posing a risk of financial, reputational, or other harm to the affected individual. A breach does NOT include:
 - a. Unintentional access to information by an employee;
 - b. Inadvertent disclosure of protected information by the Nursing Service to another party authorized to access it; or
 - c. Disclosure of information where the person to whom the disclosure was made would not be able to retain the information.
2. "Business Associate" means an outside business or organization that provides services by agreement or contract to the Nursing Service, including but not limited to billing, accounting, or transportation services.
3. "Identity Theft" means fraud committed or attempted using the identifying information of another person.
4. "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.
5. "Patient" means all customers or consumers of services provided by the Nursing Service.
6. "Protected Health Information" means personally identifiable health information.
7. "Red Flag" means a pattern, practice or specific activity that indicates possible existence of Identity Theft.

annually for approval. Updates to this Policy will then be distributed to employees and Business Associates of the Nursing Service.

7. It is the Nursing Service's Policy that all Business Associates will be contractually bound (a) to comply with FTC Red Flags Rule, any applicable state law concerning data security and this Policy, and (b) to have policies in place to detect, prevent and mitigate the risk of Identity Theft. The Compliance Officer will confirm the existence of these policies with each contact person at each Business Associate.
8. The Compliance Officer will work with the Town's Director of Information Technology to ensure that all electronically stored Protected Health Information is password protected. The Compliance Officer will also ensure that all Protected Health Information sent electronically or stored on portable devices is encrypted.

D. PROCEDURE:

1. **Identification of Red Flags:**
 - A. In the course of caring for patients, staff may encounter inconsistent or suspicious documents, information or activities that may signal Identity Theft.
 - B. The Nursing Service has identified the following Red Flags that may occur in the course of providing services:
 1. Alerts, notifications or warnings are received from a consumer or credit reporting agency, including an unusual increase in use.
 2. A complaint or question is made by a patient based on the patient's receipt of:
 - i. A bill for another individual;
 - ii. A bill for a product or service that the patient denies receiving;
 - iii. A bill from a health care provider that the patient never patronized;
 - iv. An explanation of insurance benefits (EOB) for health care services never received; or
 - v. Records indicating medical treatment inconsistent with current findings for example allergies are inconsistent.
 3. Records show medical treatment that is inconsistent with a physical examination or a medical history as reported by the patient or healthcare provider.
 4. An insurance report indicates that insurance benefits have been depleted or the lifetime cap has been reached.
 5. A patient who claims to be a victim of Identity Fraud disputes a bill.

6. A patient is unable to produce an insurance card (in conjunction with other Red Flags).
7. A notice or inquiry is received from an insurance fraud investigator for a private health insurer or a law enforcement agency, including a Medicare or Medicaid fraud agency.
8. Mail sent to the identified patient is repeatedly returned as undeliverable.
9. Inconsistent information is noted on identifying documents presented by the patient including, but not limited to:
 - i. Documents appear to have been altered or forged;
 - ii. Addresses do not match;
 - iii. Social Security numbers have not been issued or are listed on the Social Security Administration's Death Master File;
 - iv. Addresses given are typically associated with fraudulent activities such as mail drops or prison addresses;
 - v. Out of area phone numbers are provided where there is no accompanying information to explain use of such number; or
 - vi. Incomplete personal information is provided on applications.

2. **Detection of Red Flags**

- A. Any request for services made directly by a family member of a patient or potential patient must be confirmed in writing by an ordering physician.
- B. Upon first undertaking care from the Nursing Service, two forms of patient ID are required to be shown to the attending clinician: one picture ID and one health insurance card. If patient is unable to produce one of these forms of ID, confirmation of identity by another agency employee or verification from Town of Acton Town Clerk's office of residence may suffice.
- C. In reviewing ID presented, the attending clinician will look for the Red Flags identified above.
- D. An alternative procedure for confirming identity will be determined by the attending clinician and the Compliance Officer, should they be unable to utilize above methods.
- E. If the patient has received Nursing Service care previously and is known to employees, this step may be waived.
- F. If patient has not completed registration form within past six months, review form with the patient to make sure it is up to date.
- G. All Nursing Service employees will review all identifying information upon receipt from each patient to ensure that there are no inconsistencies.
- H. All Nursing Service employees are required to report any suspicion of fraud or abuse to the Compliance Officer.

3. Response to Red Flags

- A. Employees are required to immediately report all Red Flags to the Compliance Officer, along with all related documentation and complete an Unusual Occurrence Report, a sample of which is attached to this Policy as Exhibit A.
- B. All breaches of security, such as loss of laptop containing patient information must be reported to Compliance Officer immediately.
- C. If the Nursing Service employee detects any discrepancies or is unable to complete identification procedure, the employee is instructed not to raise alarm, but to record any documentation available, complete admission to the extent possible and leave the residence. The employee is not to confront anyone in their home regarding the concerns.
- D. Upon receipt of the documentation and an Unusual Occurrence Report, the Compliance Officer will review all materials and authenticate the documentation (to the extent possible) to determine whether fraudulent activity or other potential Breach has occurred.
- E. If fraudulent activity or other potential Breach is detected, the Compliance Officer will take the following steps:
 - i. Determine if a Breach has occurred (as defined in Section B.1 above).
 - a. For guidance on whether a breach has occurred, refer to the Breach Assessment Tool, attached as Exhibit B to this Policy.
 - ii. If there is a Breach,
 - a. Cancel all pending transactions.
 - b. Check the affected patient charts to make sure no fraudulent information was added to charts that may compromise patient health and safety.
 - 1. Maintain the separate chart with false or fraudulent information. This may be necessary for cross-reference to affected patient's chart and may aid in further investigation of the Breach.
 - c. Initiate the applicable notification requirements described below. [Note: The notification requirements are only triggered in the event of a Breach involving *unsecured* (meaning non-encrypted) personal information as listed in Section C.2 above.]

4. Notification Requirements in Case of a Breach:

- A. In case of a Breach, the Compliance Officer will notify the Town Manager (Steven Ledoux, 978-264-9612) and Town Counsel (Stephen Anderson, 617-621-6510), explain relevant facts and identify steps already taken in relation to Breach.

- B. Notify Acton Police Department:
- i. In case of a Breach, the Compliance Officer will call Chief of Police at (978) 264-9638 as soon as possible. The conversation with the Police Chief should cover the following:
 - a. Documents required by Police to investigate the suspicious activity. (Note: Do not provide confidential health information. Do provide information necessary to further investigation.)
 - b. Whether notification of affected patients should be delayed due to the Police investigation. If Police recommend delay, that request should be in writing and provide a rationale for delay.
- C. Notify the Affected Patient
- i. The Compliance Officer will provide written notification to the affected patient within 60 days by first class mail, *unless instructed otherwise by federal, state or local police or law enforcement officials*. Notice of any such instructions should be provided by the Nursing Service to Town Counsel.
 - ii. If the patient has asked for notification by email, provide notification by email. Nursing Service must retain a copy of all written notifications made under this rule for at least seven years.
 - iii. If the patient is deceased, the Compliance Officer will notify next of kin, if known.
 - iv. If the Nursing Service does not have contact information for 10 or more patients affected by any Breach, the Compliance Officer will post a notice of the Breach on the Nursing Service website or follow media notification procedures described below.
 - v. A sample notification letter is attached to this Policy as Exhibit C. The Compliance Officer should modify this letter as needed on a case by case basis. In any event, any notification should include:
 - a. A brief description of the Breach including the date of the Breach and the date of discovery (if it is known).
 - b. A description of the types of data or information involved:
 1. Include details about the categories of information that have been accessed or acquired (Social Security number, financial data, etc.).
 2. Do not include technical details as to how data was obtained as this may further compromise security.
 - c. A description of the possible level of threat to the affected patient.
 - d. Steps the patient can take to protect him or herself. Instructions for obtaining a credit report freeze and to obtain credit reports (as shown in the attached sample letter) and a copy of *Medical Identity Theft Response Checklist for Consumers*, which is attached to this Policy as

Exhibit D, should be included with the notice for further guidance on protective measures.

- e. A description of what Nursing Service is doing to protect the patient from further Breach and to mitigate the effects of the Breach. To the extent appropriate, alert the patient if notification was delayed due to law enforcement investigation.
- f. A method of contacting the Nursing Service to learn more about the Breach. This must be a website, email or mailing address where the public can contact the Nursing Service regarding the Breach. If the Breach includes more than 10 unidentified individuals, the Nursing Service must provide a toll-free number for this purpose.

D. Notify local media outlets, in the following circumstances:

- i. If more than 500 Massachusetts residents are affected by the Breach, the Compliance Officer will provide a press release to the media outlets listed below as soon as possible and within 60 days at the latest. The content of the press release should include the same elements as the notification to individuals but should NOT include any personal identifying information. A sample press release is attached to this Policy as Exhibit E.

ii. Media Entities and Contact Information:

- 1. Boston Globe: email press release to newstip@globe.com.
- 2. The Acton Beacon:
News Editor – Margaret Smith
978-371-5732
Email: msmith@cnc.com
Or email beacon@cnc.com
- 3. Channel 4 (WBZ):
WBZ-TV
1170 Soldiers Field Road
Boston, MA 02134
- 4. Channel 5 (WCVB):
Andrew Vrees, News Director
WCVB-TV
5 TV Place
Needham, Massachusetts 02494
- 5. Channel 7 (WHDH): Email: email press release to newstips@whdh.com.

6. Channel 25 (WFXT):
Paul McGonagle, VP, News Director
WFXT-TV FOX25
25 Fox Drive
Dedham, MA 02027-2563

7. WBZ 1030: email press release to
wbzradionews@wbz1030.com

E. Notify the United States Secretary of Health and Human Services in the following circumstances:

- i. If more than 500 people are affected by the Breach, the Compliance Officer will fill out the electronic form available at <http://transparency.cit.nih.gov/breach/index.cfm> within 60 days of Breach.
- ii. If fewer than 500 people are affected by the Breach, the Compliance Officer will document the Breach in the attached Breach Information Log (Exhibit F). The Compliance Officer will then fill out an electronic form for each breach using the form available at <http://transparency.cit.nih.gov/breach/index.cfm> by February 28 of the year following the calendar year in which the Breach occurred.

F. Notify State Officials:

- i. The Compliance Officer will provide a notice to the following as soon as possible after the Breach:
 1. Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
 2. Ms. Barbara Anthony
Undersecretary
Office of Consumer Affairs and Business Regulation
("OCABR")
10 Park Plaza –Suite 5170
Boston, MA 02116
- ii. The notification to the Attorney General and the Undersecretary (also known as the "Director") should include:
 - a. A description of the nature of the Breach;
 - b. The number of Massachusetts residents affected; and

- c. A description of the steps the Nursing Service has taken or plans to take relating to the Breach, including steps taken in order to comply with the HIPAA Breach Notification Rule, the Red Flags Rule, and any other applicable law.
 - iii. Sample notices to the state officials are attached to this Policy as Exhibit G.
 - iv. The Office of Consumer Affairs and Business Regulation will notify the Nursing Service of relevant consumer reporting agencies or state agencies that should be contacted. After OCABR provides that information, the Nursing Service should provide a copy of the state notices to the identified agencies.
- G. If a patient detects fraudulent activity on an insurance policy or credit account and notifies Nursing Service, the Compliance Officer and Nursing Service will take the following steps:
- i. Encourage patient to file a police report.
 - ii. Encourage patient to complete the *ID Theft Affidavit*, attached to this Policy as Exhibit H and compile supporting documentation.
 - iii. Compare patient's documentation with personal information in Nursing Service records.
 - iv. Immediately cease all billing related to the claim in question pending resolution of the question of fraudulent activity.
 - v. Determine if there is a breach and follow steps for law enforcement, HHS, media, and state agency notification outlined above.

5. **Training**

- A. Staff training will be conducted for all employees, officials and contractors who may come into contact with accounts or personally identifiable information that may constitute a risk to the municipality or the Nursing Service patients. Such employees include employees performing the following tasks:
 - i. Data entry, coding, or billing;
 - ii. Handling of charts, referrals, prescriptions or other medical documents;
 - iii. Contracting or coordination with outside service providers; and
 - iv. Compliance review for this Policy.
- B. The Compliance Officer is responsible for ensuring all employees and contractors conducting the above tasks are properly trained.
- C. Employees must receive annual training in all elements of this Policy. Information covered during the annual training will be included in the orientation of newly hired employees.
- D. The Compliance Officer will request documentation of training performed or received by Business Associates.

- E. To ensure maximum effectiveness, employees will receive additional training as changes to the program are made. Employees and Contactors will receive a copy of any updates to this Policy.
- F. Employees will receive a copy of this Policy as part of any annual training. New employees will receive a copy of this Policy during their orientation.
- G. Employees who fail to comply with this Policy are subject to sanction as provided by law.

6. Periodic Updates to Plan

- A. This Policy will be reevaluated annually by the Compliance Officer to determine whether the program is up to date and applicable given the Nursing Service's practices and the Town of Acton's Master Identity Theft Policy.
- B. Periodic reviews will include an assessment of whether new accounts are covered by this Policy and whether existing accounts are susceptible to new forms of Identity Theft.
- C. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the Town and the Nursing Service employees or patients.
- D. The Compliance Officer will provide a written report on an annual basis to the Board of Health and Town Manager on the effectiveness of the current Policy and recommended changes for the upcoming year.
- E. Revisions to this Policy will be approved by the Board of Health and Board of Selectmen prior to the annual training and signed by the following:
 - i. Chairperson of Board of Health;
 - ii. Chairperson of Board of Selectmen; and
 - iii. Administrator of Nursing Service and Compliance Officer (if different).

7. Oversight of Arrangements with Business Associates

- A. The Compliance Officer will ensure that the activities of all Business Associates are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
- B. As of February 22, 2010, the Business Associates listed in Exhibit I currently provide services to the Nursing Service and may have access to the personal data listed in Section C.2. above.
- C. Within 30 days of approving this Policy and each January thereafter, the Compliance Officer will request a letter from each Business Associate:
 - i. Certifying compliance with the FTC Red Flag Rule, HIPAA Regulations, including the Breach Notification Rule, and Massachusetts Data Privacy rules (if applicable);

- ii. Certifying that the Business Associate understands that it is required to notify the Nursing Service of any Breach upon discovery of the Breach; and
 - iii. Providing a description or copy of the written information security program followed by the Business Associate.
- D. The Compliance Officer will review policies of all Business Associates to ensure that they are effective in preventing Identity Theft.
- E. The Compliance Officer will provide a copy of this Policy to all Business Associates with a letter requesting that it be followed to the extent it is more stringent than the Business Associates' own policies.
- F. When entering into agreements with new Business Associates or renewing existing contracts, the Nursing Service will ensure that the agreement requires compliance with this Policy.

E. APPROVAL AND EFFECTIVE DATE

1. This Policy will take effect immediately upon its approval by the Nursing Service Administrator in consultation with the Group of Professional Personnel, the Board of Health, and the Board of Selectmen.
2. Approval is documented below.

APPROVED:

**NURSING SERVICE
ADMINISTRATOR:**

The foregoing Policy was approved by vote of the Group of Professional Personnel at a meeting on April 10, 2012.

By: Heather Hurley

ACTON HEALTH DIRECTOR:

The foregoing Policy was approved by vote of the Board of Health at an open meeting on April 10, 2012.

By: Douglas Halley

ACTON BOARD OF SELECTMEN:

The foregoing Policy was approved by vote of the Board of Selectmen at an open meeting on _____, 2012.

By: Janet Adachi, Clerk

EXHIBITS

EXHIBIT	DESCRIPTION
A	Unusual Occurrence Report
B	Breach Assessment Tool
C	Draft Patient Notification Letter
D	<i>Medical Identity Theft Response Checklist for Consumers</i>
E	Draft Press Release
F	Sample of Breach Information Log
G	Draft Notification Letter to State Officials
H	Sample of <i>ID Theft Complaint and Affidavit</i>
I	List of Business Associates